Altiris® HP Client Manager 6.1 SP1 Release Notes

May 4, 2006

NOTICE

The content in this document represents the current view of Altiris as of the date of publication. Because Altiris responds continually to changing market conditions, this document should not be interpreted as a commitment on the part of Altiris. Altiris cannot guarantee the accuracy of any information presented after the date of publication.

© 2006 Altiris, Inc. All rights reserved.

Altiris, the Altiris logo, BootWorks, Inventory Solution, LabExpert, PC Transplant, RapiDeploy, and RapidInstall are registered trademarks of Altiris, Inc. in the United States.

Carbon Copy is a registered trademark licensed to Altiris, Inc. in the United States and a trademark of Altiris, Inc. in other countries.

Altiris eXpress, Deployment Server, Deployment Solution, My IT Forum, Notification Server, Vision, Web Reports and other product names are trademarks of Altiris, Inc. in the United States and other countries.

All other brand names are trademarks or registered trademarks of their respective companies.

Information in this document is subject to change without notice. For the latest documentation, visit our Web site at www.altiris.com.

Contents

1 Overview 2
2 Supported Computers and Platforms 3
3 Installation and Licensing 6
4 New Features in this Release 7
5 Feature Enhancements in this Release 9
6 Known Issues 10

1 Overview

1.1 Document Purpose

This document provides the "what's new" and "known issues" information for the 6.1 SP1 release of Altiris® HP Client Manager.

1.2 Background

HP Client Manager (HPCM, formerly known as HP Client Manager Software - HPCMS) is a free hardware management tool for HP client computers. This tool provides in-depth client inventory, driver and utility updating, remote BIOS management, remote Embedded Security management, hardware monitoring, diagnostics, and problem resolution. HP Client Manager integrates with Altiris® Client Management Suite, Altiris® HP OpenView, Altiris® HP Systems Insight Manager, and Microsoft Systems Management Server (SMS).

1.3 Documentation

Product documentation for version 6.1 SP1 is available in the HP Client Manager Product Guide (*HPCM.pdf* and *HPCM.chm*). To view Altiris product documentation in .PDF format, use Adobe Acrobat Reader (available at: http://www.adobe.com/products/acrobat/readstep2.html).

2 Supported Computers and Platforms

2.1 Supported HP Computers

The following table lists the HP commercial computers that are tested and supported by HP Client Manager 6.1 SP1. Additionally, the computers must be running one of the supported operating systems. For more information, see Supported Operating Systems.

Desktops	**Supports Embedded Security**
Compaq Evo D330	No
Compaq Evo D530	Yes
Compaq Evo D300	No
Compaq Evo D500	No
Compaq Evo D300 Small Form Factor	No
Compaq Evo D500 Slim Tower	No
Compaq Evo D310 Small Form Factor	No
Compaq Evo D510 Small Form Factor	No
Compaq Evo D310v	No
Compaq Business Desktop D315	No
Compaq Evo D320	No
Compaq Business Desktop D325 Slim Tower	No
Compaq Business Desktop D325 Microtower	No
HP Compaq Business Desktop dx6050 Microtower	No
Compaq Evo D500 Ultra-slim Desktop	No
Compaq Evo D500 Small Form Factor	No
Compaq Evo D500 Ultra-slim Desktop	No
Compaq Evo D510 Ultra-slim Desktop	No
Compaq Evo D510 Small Form Factor	No
Compaq Evo D510 e-pc	No
Compaq D530 Ultra-slim Desktop	Yes
HP Compaq dc5000	No
HP Compaq dc5100 Microtower PC	No
HP Compaq dc5100 Small Form Factor PC	No
HP Compaq dc7100 Ultra-slim Desktop	Yes
HP Compaq dc7100 Convertable Minitower	Yes
HP Compaq dc7100 Small Form Factor	Yes
HP Compaq dx6100 Slim Tower	No
HP Compaq dc7600 Ultra-slim Desktop	Yes

HP Compaq dc7600 Small Form Factor	Yes
HP Compaq dc7608 Small Form Factor	Yes
HP Compaq dx7200 Slim Tower Business PC	Yes
HP Compaq dx7208 Slim Tower PC	Yes
HP Compaq dc7600	Yes
HP Compaq dc7608 Convertible Minitower	Yes
HP Compaq dx5150 Microtower PC /Slim Tower/Small Form Factor	No
HP Compaq dx6100 Microtower	No
HP Compaq dx6120 Microtower	No
HP Compaq dx6120 Slim Tower	No
HP Compaq rp5000	No
HP e-PC	No
HP Compaq dx7200/dx7208 Micro Tower Business PC	Yes
Workstations	**Supports Embedded Security**
HP workstation xw4000	No
HP Workstation xw4100	No
HP Workstation xw4200	Yes
HP Workstation xw4300	Yes
HP Workstation xw5000	No
HP Workstation xw6000	No
HP Workstation xw6200	No
HP workstation xw8000	No
HP Workstation xw8200	No
HP Workstation xw9300	No
HP Compaq Workstation w6000	No
Notebooks and Tablet PCs	**Supports Embedded Security**
Compaq Evo N610c	No
Compaq Evo N620c	No
Compaq Evo N800v/N800c	No
Compaq Evo N1000	No
HP Compaq Business Notebook nc4000/nc4010	Yes
HP Compaq nc4200 Notebook PC	Yes
HP Compaq Business Notebook nx5000	No
HP Compaq Business Notebook nc6000	Yes
HP Compaq nc6220 Notebook PC	Yes
HP Compaq nc6230 Notebook PC	Yes

HP Compaq Business Notebook nc8000	Yes
HP Compaq nc8220 Notebook PC/HP Compaq nc8230 Notebook PC	No
HP Compaq nc6120 Notebook PC	No
HP Compaq Nx6120/nc6140/nc6110 Notebook PC	No
HP Compaq Mobile Workstation NW8000	Yes
HP Compaq Mobile Workstation nw8240	Yes
Compaq Tablet PC TC1000	No
Compaq Tablet PC TC1100	No

Note: Newer models not listed are probably supported.

2.2 Supported Operating Systems

- Windows XP Professional
- Windows 2000 Professional
- Windows XP Tablet Edition
- Windows XP Professional x64 Edition *

*x64 systems do not support Diagnostics, System Health Scan, and Management of Embedded Security.

2.3 Discontinued HP Computer Support

Desktops	
Compaq Deskpro EN, EX/EXS Series	
Compaq iPAQ Desktop	
Workstations	
Deskpro Workstation AP 250	Evo Workstation W6000
Deskpro Workstation AP 300	Evo Workstation W8000
Professional Workstation AP200	HP Workstation x1000
Professional Workstation AP400	HP Workstation x1100
Professional Workstation AP550	HP Workstation x2000
Professional Workstation SP700	HP Workstation x2100
Professional Workstation SP750	HP Workstation x4000
Evo Workstation W4000	
Notebooks and Tablet PCs	
Compaq Evo N800w	Compaq Armada M300 Family
Compaq Evo N1005	Compaq Armada M700 Family
Compaq Evo N1020	HP Omnibook 6100
Compaq Evo n400c/410c	HP Omnibook XE4000
Compaq Evo n600c	HP Omnibook XE-GF

Note: Systems supported in previous versions of HPCM and are not listed in current version of Supported HP system list are probably retired in the current version.

2.4 List of computers that require BIOS upgrade to become HPCM Embedded Security Manageable

The following models are currently not manageable by HPCM due to partial support for remote management of Embedded Security [TPM]:

- nw9440
- nc8430
- nw8440
- nc6320
- nc6400
- nc4400
- tc4400
- nc2400

These notebook PCs require an upgrade to the system BIOS to fully support remote management of Embedded Security chip [TPM]. Until the BIOS upgrades are available, these systems will be unsupported by HP Client Manager.

It is expected that the BIOS updates will be available for these systems in the summer of 2006. When available, the BIOS upgrades can be automatically deployed to these systems, thus enabling them to fully support remote management of Embedded Security.

3 Installation and Licensing

Installation and licensing information is provided in the HPCM documentation, the Readme – Quick Install.PDF file (included in the solution .ZIP file downloaded from the Altiris Web site), the Altiris Getting Started Guide, and the Altiris® Notification Server™ Reference Guide.

3.1 Upgrading to HPCM 6.1 SP1

3.1.1 Upgrade Recommendations

If you currently have HPCM 6.1 installed, we recommend upgrading to HPCM 6.1 SP1 rather than uninstalling HPCM 6.1 and then installing HPCM 6.1 SP1. If you uninstall HPCM 6.1, your existing data and custom packages, collections, and so forth will be lost. To upgrade from HPCM 6.1 to HPCM 6.1 SP1, simply install HPCM 6.1 SP1 over the existing HPCM 6.1.

Important: While upgrading to HPCM 6.1 SP1, you should not have any HPCM 6.1 tasks running or scheduled to run. Disable all events that are scheduled to run ASAP or during the next hour or so until the upgrade completes. If the HPCM 6.1 server or HPCM 6.1 clients are in the process of executing a task, the upgrade to HPCM 6.1 SP1 may not complete successfully.

3.1.2 Notification Policies

During an upgrade from HPCM 6.0 or 6.1 to HPCM 6.1 SP1, any modified Notification Policy actions that are part of the standard set of installed Notification Policies and their settings are not upgraded. Any customer created Notification Policies are saved. However, due to changes in the way HPCM detects health of client computers, custom Notification Policies that were created in HPCM 6.0 or 6.1 may not be applicable in HPCM 6.1 SP1. You will have to re-create these policies in HPCM 6.1 SP1.

3.1.3 Collections

All collections are retained during the upgrade from HPCM 6.0 or 6.1 to HPCM 6.1 SP1. However, during an upgrade from HPCM 6.1 to HPCM 6.1 SP1, any collection that uses NT 4.0 or Windows 98 is not valid in 6.1 SP1 because NT 4.0 and Windows 98 are not supported.

HPCM installations that upgrade to HPCM 6.1 SP1 may retain the collection, "Windows 2000 Servers". This collection should not be used in HPCM 6.1 SP1 for client systems because it is not a client OS. Windows 2000 Server is a supported OS for the Notification Server.

3.1.4 Custom Reports

During an upgrade from HPCM 6.0 to 6.1 SP1, or from HPCM 6.1 to 6.1 SP1, custom reports may not be retained. If you want to retain custom reports, we recommend exporting the reports to a safe location and then importing them after the upgrade. However, because the inventory and diagnostics tables change after the upgrade, the reports will not contain updated historical data.

3.1.5 SoftPaq and BIOS Administration Policies/Packages

Existing SoftPaq policies/packages and BIOS administration policies/packages created in HPCM 6.0 are retained in HPCM 6.1 SP1. However, both the policies and the packages are listed under the respective Tasks folder. For example, a SoftPaq policy/package created in HPCM 6.0 is retained in HPCM 6.1 SP1, but it is listed under HP SoftPaq Delivery\HP SoftPaq Delivery Tasks folder. In HPCM 6.1 SP1 all new SoftPaq and BIOS changes have their respective policies and tasks displayed in separate folders.

3.1.6 Health Monitoring Settings

During an upgrade from HPCM 6.0 or 6.1 to HPCM 6.1 SP1, health monitoring settings retain only the global enable/disable setting. Individual selections of enable/disable for specific hardware items are not retained due to changes in Health monitoring in 6.1 SP1.

3.1.7 Non-default HP SoftPaq Filestore Path must be reconfigured

The HP SoftPaq Filestore has the following default path:

C:\Program Files\Altiris\Notification Server\NSCap\Bin\Win32\X86\HPCMS\Filestore

If you are using a non-default path, you must reconfigure your custom path after you perform the upgrade. For information on how to configure the HP SoftPaq Filestore path, refer to the *HPCM Product Guide.*

3.1.8 Issues when upgrading from HPCMS 5.6 SP1 to HPCM 6.1 SP1

Notification Server 5.5 should be upgraded to Notification Server 6.0 SP3 before you install HPCM 6.1 SP1. To ensure that HPCM 6.1 SP1 works properly, all Notification Server clients should be upgraded to the Notification Server 6.0 SP3 Altiris Agent prior to HPCM 6.0 being installed. HPCM 6.1 SP1 should not be installed on Notification Server 5.5 because HPCM is not supported on Notification Server 5.5.

4 New Features in this Release

4.1 Manage Embedded Security

HPCM 6.1 SP1 provides various features to manage Embedded Security on client computers. These include archiving the Embedded Security credentials and settings, and managing the state of Embedded Security. These features are provided with the help of HP Embedded Security Tasks and an Embedded Security Wizard.

Note: Before using the Embedded Security (TPM) features in HPCM, we recommend that you read the HP ProtectTools Security Manager Guide to gain an understanding of how Embedded

Security works. This guide can be found on the HP Web site for each model: http://www.hp.com/.

The following tasks are provided with the Embedded Security feature:

4.1.1 Initialization of Embedded Security

HP Client Manager lets an administrator initialize Embedded Security for the client computer, which can further be managed with the help of the HP Client Manager Agent. This feature initializes the Embedded Security by enabling and taking ownership of the TPM (Trusted Platform Module) chipset. The TPM chipset is the device that enables the usage of Embedded Security features on client computers.

4.1.2 Modify Embedded Security Owner password

This feature helps an administrator modify an Embedded Security Owner password.

4.1.3 Create Password Reset Token file [Manage Security User passwords]

This feature lets an administrator create password reset token information, which is further used to generate a "password reset secret code."

4.1.4 Reset Security User Password [Manage Security User passwords]

This feature lets an administrator generate a "password reset secret code" for a client computer. This code is used to reset the Embedded Security password of a user on the client computer.

4.1.5 Archive Embedded Security

This feature helps an administrator archive Embedded Security credentials and settings. In case of a disaster, the administrator can use this archive to restore the Embedded Security credentials and settings on the client computer.

4.1.6 Restore Embedded Security

This feature lets the administrator restore Embedded Security credentials and settings.

4.1.7 Embedded Security Wizard

This feature helps an administrator create Embedded Security related policies using the wizard.

5 Feature Enhancements in this Release

5.1 Improved Serial and Parallel port data

HPCM now provides additional data about Serial and Parallel ports, which includes information on Interrupt, DMA channel, connector type, and port type.

5.2 Information related to PCI slots

HPCM provides information about PCI slots, which includes information on Slot Designation, Current Usage, and Maximum Data Width.

5.3 Information related to Memory slots

HPCM now provides information about Memory slots, which includes the total number of memory slots present and number of used memory slots.

5.4 Improved Disk Drive data

HPCM now provides additional data about disk drives, which includes the Serial number, Version, and Manufacturer of the disk drive.

5.5 Improved battery data

HPCM now provides detailed information related to columns already present in the battery information. The following descriptive information is provided: Availability, BatteryStatus, Chemistry, DesignCapacity, and DesignVoltage.

5.6 Improved monitor data

HPCM now provides additional data about monitors including the monitor serial number.

6 Known Issues

6.1 Hot-swapping devices on clients are not detected until restart

You can configure the Health monitor on the Altiris Console by clicking the **Configuration** tab, and, in the left pane, selecting **Solution Settings > Platform Administration > HP Client Management > HP Health Client Monitoring**. The "Battery changed," "Disk drive changed," and "Monitor changed" settings are associated with "On device changed event." This setting implies that HPCM will probe for a device change when it receives a Plug and Play (PnP) notification from the system. Due to issues where a Plug and Play notification does not work properly, these probes only occur "Once at boot."

6.2 Swapping batteries of the same capacity may not be detected

The serial numbers of some batteries on some computers cannot be determined. In such cases, the capacity of the batteries differentiates between battery changes. If the capacities of such batteries are equal, a device change cannot be determined, and an event is not sent.

6.3 Swapping memory sticks of the same capacity may not be detected

The serial numbers of some memory sticks on some computers cannot be determined. In such cases, the capacity and speed of the memory sticks are used for differentiation. If the capacity and speed are equal, a device change cannot be determined, and an event will not be sent.

6.4 Enabling Wake on LAN requires configuration of the Altiris Agent Settings

To enable Wake on LAN for HP Client Manager SoftPaq delivery, BIOS Administration, Inventory, and Diagnostics, the user must enable the power management feature on the client computer.

To enable power management,

1. From the Altiris Console, click the **Configuration** tab.
2. In the left pane, select **Configuration > Altiris Agent > Altiris Agent Configuration**.
3. Click **All Desktop Computers (excluding 'Package Servers')**.
4. Click the **Advanced Settings** tab.
5. Select the **Enable power management on Altiris Agent** checkbox.
6. Click **Apply**.

When HP client computers are updated with the new Altiris Agent settings, they will be correctly configured to recognize and respond to Wake on LAN packets.

6.5 Certain BIOS settings do not take affect until a restart is enabled

HP recommends restarting your client computer after you make a BIOS change. For example, on HP computers manufactured after 2002, the enabling or disabling Wake on LAN or the Hood Lock will not engage until the client computer is restarted. Therefore, to ensure that BIOS changes have been implemented, restart the client after the BIOS package has been installed.

6.6 Multi-Language Support Report Data

The HP Client Manager Agent does not support regional languages. Information reported by the agent is in English and it is saved in the same language in the HPCM database. Reports showing this information may have names and column headings in regional languages, but content (data) in the report is always displayed in English.

6.7 Computers that do not support BIOS modifications

The following HP legacy computers were designed such that BIOS changes cannot be made using HP Client Manager.

- HP e-PC
- HP Workstations xw5000
- HP Workstations xw8000
- HP Compaq dx5150 (to a limited extent)
- Compaq Tablet PC tc1000 series
- Compaq Tablet PC tc1100 series

6.8 HP Instant support diagnostic tools limitations

HP Instant Support diagnostic tools do not currently support client computers running Windows XP Embedded or XP Professional x64.

6.9 Limited Support for Windows XP Professional x64

HPCM 6.1 SP1 includes SSM 2.0, which supports driver updates under Windows XP Professional x64 as well as BIOS flashing, BIOS changes, and driver installation.

6.10 Task Limitations for Windows XP64 computers

Windows XP64 bit computers do not support the following tasks: "HP Instant Support Diagnostics" and "HP Instant Support System Health Scan". Presently, these tasks are only supported under Windows 32bit Operating Systems.

6.11 Inventory Limitations for Windows XP64 computers

The inventory of BIOS settings on a system running Windows XP64 requires the system to have HP Client Management Interface native in the BIOS. BIOS Inventory items are not available on systems running WinXP64 without the HP Client Management Interface native in the BIOS (for example, HP dx5150 desktop). Systems running Windows XP32 will be able to gather the inventory of BIOS settings with or with out the HP Client Manager Interface native in the ROM.

6.12 Embedded Security (TPM) and XP64 bit systems

Embedded Security (TPM) is not supported on Windows XP64 bit systems. Therefore, if any TPM related task is executed on Windows XP64 platform, it will fail. When TPM is supported on Windows XP64 bit systems in the future, the administrator will be able to remotely manage those systems since those systems will automatically become a TPM supported platform.

6.13 Battery Level Threshold reporting below -1 percent

The following alert means that the battery is reporting odd or irregular data: "HP Client Manager has detected that your battery level threshold is below -1 percent."

6.14 Reject Initialization

On certain notebooks (for example, nc6220), the Embedded Security option to allow users to reject initialization does not work. A future update to the ROM BIOS will correct this issue.

6.15 TPM Feature Limitations

On the HP d330 and HP dc7100 desktops with Embedded Security (TPM) version 1.1b, the following Embedded Security features are not supported: a) 'Manage security User passwords' and b) 'Manage security credentials and Settings: Archive and Restore'. However, with the same version of TPM, the above listed features are supported on notebooks such as the nc6220.

6.16 Inventory and WMI

Computer inventory along with Embedded Security related inventory may not work properly if there is problem in the WMI service of the operating system. Try rebooting the client.

6.17 "Hidden TPM"

HPCM inventory will not gather TPM inventory if the TPM chip is set to "hidden" in the BIOS.

6.18 HPCM QuickStart Availability

In some cases, the installed HPCM settings may take time to be reflected in the Notification Server. As a result, the HPCM QuickStart page may not automatically open properly immediately after installation for about one minute. For this reason, the HPCM QuickStart page can be accessed through the Start menu by clicking **Start > Programs > Altiris > Quick Starts > HP Client Manager**. There is also an HPCM QuickStart shortcut available on the Desktop.

6.19 Monitor Change Alerts

On some systems, due to unsynchronized information received from the operating system for a connected monitor, phantom monitor change alerts can be displayed. These alerts can also happen due to an improper serial number gathered for a monitor.

6.20 Failed SoftPaq Downloads

If System Health Scan encounters a problem downloading SoftPaqs from HP, it can cause HPCM to think that all SoftPaqs were downloaded successfully. This can cause empty SoftPaq packages to be created. If you encounter failed downloads via System Health Scan, download the desired SoftPaqs from www.hp.com/suppport and manually place them into the Filestore directory (not in a subdirectory within the Filestore.) Rebuild the Filestore and then use the SoftPaq wizard to deploy the SoftPaqs. Use the Notification Server error log to confirm if SoftPaqs were downloaded successfully. Then view the Notification Server (NS) error log using the following steps: a) click on the Configuration tab in the NS Console page b)Expand Server Settings \ Notification Server Settings c) click on Error Logging d) click on the View Status Messages button to view the NS error log.

6.21 SoftPaq File Locations

The SoftPaq Wizard cannot handle SoftPaqs that are located in subdirectories under the main Filestore directory. The download directory is used only by System Health Scan. It is recommended that you do not manually place any SoftPaqs into this download directory.

6.22 Duplicate SoftPaqs

Before downloading a SoftPaq through a System Health Scan, confirm that you do not already have the SoftPaq in your Filestore. Duplicate SoftPaqs can cause a SQL error when updating the Filestore.

6.23 Mouse Response

Microsoft recently changed the operation of their ActiveX controls which may result in some HPCM pages requiring two mouse clicks before a pointer changes. This will be addressed by a future update of Notification Server.

6.24 Incorrectly Formatted Information

On some systems (i.e. HP dc7200 desktop and HP dc7600 desktop), due to problems with BIOS, incorrectly formatted information is gathered and reported to the Notification Server This can also affect the information displayed through the 'HP BIOS Advanced Administrator wizard', 'HP Tool Update Wizard' and 'HP BIOS Report'. A new ROM BIOS from HP as well as an Advanced BIOS Wizard cleaning utility will be released to address this issue.

6.25 Incorrect Reported Disk Size

In the resource manager, the reported disk size is not reported correctly through WMI (HPCMS_WMI_Win32_DiskDrive). The correct size for hard disk is located in HPCMS_WMI_Win32_LogicalDisk.

6.26 Disk Drive Threshold Alerts Description Error

In the Health Alert Policy, "Disk Drive Threshold Alerts", the description provided for "Send E-Mail" incorrectly states the alert is for a memory module alert.

6.27 "Windows 2000 Servers" Collection Usage

HPCM installations that upgrade to HPCM 6.1 SP1 may retain the collection, "Windows 2000 Servers". This collection should not be used in HPCM 6.1 SP1 for client systems because it is not a client OS. Windows 2000 Server is a supported OS for the Notification Server.

6.28 Wake-on-Lan Scheduling Limitations

In some environments, due to limitations of Notification Server, the WOL option of schedule is not working as expected. Ensure you have at least two clients per subnet for WOL proxies to work.

6.29 HP BIOS Report Wizard

The HP BIOS Report Wizard does not work properly if you create a report that joins multiple selections using "OR". The use of "AND" to join works properly.

6.30 Anti-virus Agents and Java Scripts

HP Insight Manager System Health Scan executes java scripts. If you have virus detection software that is blocking java scripts from executing you will need to allow the following java scripts the ability to execute:

- defrag.js (executes to see if the client needs to be defragged)
- parasite.js (executes to see if spyware is loaded on the client).